

Exhibit 5

United States District Court

EASTERN

DISTRICT OF

NEW YORK

In the Matter of the Search of
(Name, address or brief description of person or property to be searched)

THE ITEMS DESCRIBED IN ATTACHMENT A

SEARCH WARRANT

CASE NUMBER:

13 M290

TO: Special Agent Aaron Spivack and any Authorized Officer of the United States

Affidavit(s) having been made before me by Special Agent Aaron Spivack who has reason to
Affiant

believe that ☐ on the person of or ☒ on the premises known as (name, description and/or location)

The items described in Attachment A.

in the EASTERN District of NEW YORK there is now concealed a certain
person or property, namely (describe the person or property)

The items described in Attachment B.

I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before April 14, 2013
Date

(not to exceed 14 days) the person or place named above for the person or property specified, serving this warrant and making the search (in the daytime - 6:00 A.M. to 10:00 P.M.) (at any time in the day or night as I find reasonable cause has been established) and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to Duty Magistrate as required by law.

United States Judge or Magistrate Judge

April 1, 2013 at 12:45 PM at Brooklyn, New York
Date and Time Issued City and State

Hon. Robert M. Levy, U.S.M.J.
Name and Title of Judicial Officer

Robert Levy
Signature of Judicial Officer

ATTACHMENT A

Property to be Searched

The SUBJECT ITEMS are ONE APPLE LAPTOP, SERIAL NO. 7393759V7XJ ("SUBJECT ITEM 1"), ONE SONY DIGITAL CAMERA, SERIAL NO. 0124465 ("SUBJECT ITEM 2"), ONE 8GB SD CARD ("SUBJECT ITEM 3"), ONE USB MEMORY STICK ("SUBJECT ITEM 4"), and ONE BLACK APPLE IPHONE ("SUBJECT ITEM 5"), ONE WHITE APPLE IPHONE ("SUBJECT ITEM 6"), ONE 32 GB SD CARD ("SUBJECT ITEM 7"), ONE SKY LINK CDMA MODEM ("SUBJECT ITEM 8"), ONE SONY DIGITAL CAMERA, SERIAL No. 7080101 ("SUBJECT ITEM 9"), ONE GREY NOTEBOOK, WITH COVER READING "SECRET MAGIC SPELLS" ("SUBJECT ITEM 10"), and ONE 4 GB SD CARD ("SUBJECT ITEM 11") (collectively referred to as the "SUBJECT ITEMS")

ATTACHMENT B

Particular Things to be Seized

ITEMS TO BE SEIZED FROM THE SUBJECT ITEMS, all of which constitute evidence or instrumentalities of violations of Title 18, United States Code Sections 2241(c), 2251, 2252, 2252A and 2422(b) :

1. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the production, possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2251, 2252 and 2252A, in any form wherever they may be stored or found;

2. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

3. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

4. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:

a. correspondence, including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or relating to the enticement of minors to engage in illegal sexual activity; and

b. ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

5. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.

6. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

7. Records or other items which evidence ownership or use of computer related equipment, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

8. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct or the enticement of minors to engage in illegal sexual contact.

9. Address books, names, lists of names and addresses of individuals believed to be parents or guardians of minors.

10. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be parents or guardians of minors.

11. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.

12. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

13. All documents, text messages, "chat," or instant messages, call logs, and any other electronically-stored data (whether on cellular telephones or elsewhere) relating to conspiracy to produce child pornography or attempts to produce child pornography or enticement of minors to engage in illegal sexual contact or aggravated sexual abuse of children.

14. Evidence of who used, owned, or controlled any of the SUBJECT ITEMS at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence. User attribution information (i.e. files and other data such as chats or e-mails) relevant to the trading of child pornography. Such information tends to show the identity of the person using the computer near the time of the criminal activity;

15. Evidence of software that would allow others to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

16. Evidence of the lack of such malicious software;

17. Evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;

18. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;

19. Evidence of the times the SUBJECT ITEMS were used;
20. Passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT ITEMS;
21. contextual information necessary to understand the evidence described in this attachment.

If any materials protected by the Privacy Protection Act, 42 U.S.C. § 2000aa are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

22. Records and things evidencing the use of any IP address, including:
 - a. records of Internet Protocol addresses used;
 - b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections , 2241(c), 2251, 2252, 2252A and 2422(b).

Definitions

- a. "Child Erotica," as used herein, means materials and items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene and that do not necessarily depict minors in sexually explicit poses or positions.
- b. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer generated image that is, or is

indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital, oral genital, or oral anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); and peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as

cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. "IP Address" as used herein, the IP Address or Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

j. "Wireless telephone": A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

k. "Digital camera": A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

l. "Portable media player": A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include

various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

p. "GPS": A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

q. "PDA": A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and

presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

r. "Tablet": A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

s. "Pager": A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

t. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

SLT:TJS

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- against -

THE ITEMS KNOWN AND DESCRIBED:

- A. ONE APPLE LAPTOP, SERIAL
NO. 7393759V7XJ
- B. ONE SONY DIGITAL CAMERA,
SERIAL NO. 0124465
- C. ONE 8GB SD CARD
- D. ONE USB MEMORY STICK
- E. ONE BLACK APPLE IPHONE
- F. ONE WHITE APPLE IPHONE
- G. ONE 32 GB SD CARD
- H. ONE SKY LINK CDMA MODEM
- I. ONE SONY DIGITAL CAMERA,
SERIAL No. 7080101
- J. ONE GREY NOTEBOOK, WITH
COVER READING "SECRET MAGIC
SPELLS"
- K. ONE 4 GB SD CARD

(COLLECTIVELY, THE "SUBJECT
ITEMS")

13 M2 90

AFFIDAVIT IN SUPPORT
OF SEARCH WARRANT

(T. 18, U.S.C., §§ 2241(c),
2251, 2252, 2252A and
2422(b))

EASTERN DISTRICT OF NEW YORK, SS:

AARON SPIVACK, being duly sworn, deposes and states
that he is a Special Agent with the Federal Bureau of
Investigation ("FBI"), duly appointed according to law and
acting as such:

Upon information and belief, there is probable cause to believe that there is kept and concealed within THE ITEMS KNOWN AND DESCRIBED AS: ONE APPLE LAPTOP, SERIAL NO. 7393759V7XJ ("SUBJECT ITEM 1"), ONE SONY DIGITAL CAMERA, SERIAL NO. 0124465 ("SUBJECT ITEM 2"), ONE 8GB SD CARD ("SUBJECT ITEM 3"), ONE USB MEMORY STICK ("SUBJECT ITEM 4"), and ONE BLACK APPLE IPHONE ("SUBJECT ITEM 5"), ONE WHITE APPLE IPHONE ("SUBJECT ITEM 6"), ONE 32 GB SD CARD ("SUBJECT ITEM 7"), ONE SKY LINK CDMA MODEM ("SUBJECT ITEM 8"), ONE SONY DIGITAL CAMERA, SERIAL No. 7080101 ("SUBJECT ITEM 9"), ONE GREY NOTEBOOK, WITH COVER READING "SECRET MAGIC SPELLS" ("SUBJECT ITEM 10"), and ONE 4 GB SD CARD ("SUBJECT ITEM 11") (collectively referred to as the "SUBJECT ITEMS"), the items described in Attachment A to this affidavit, all of which constitute evidence or instrumentalities of the possession, access with intent to view, transportation, receipt, distribution, reproduction attempted production and conspiracy to produce sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2241(c), 2251, 2252, 2252A, and 2422(b).

The source of my information and the grounds for my belief are as follows:¹

AGENT BACKGROUND

1. I have been employed as a Special Agent with the FBI since 2008 and am currently assigned to the New York Office. For approximately three years, I have been assigned to a Crimes Against Children squad. I have been assigned to investigate violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through training in classes and daily work related to conducting these types of investigations. I have participated in a number of investigations into the receipt, possession, and/or distribution of child pornography by electronic means, as well as the sexual enticement of minors. As part of my responsibilities, I have been involved in the investigation of numerous child pornography cases and have reviewed hundreds of photographs depicting children (less than eighteen years of age) being sexually exploited by adults. Through my experience in these

¹ Because the purpose of this Affidavit is to set forth only those facts necessary to establish probable cause to search, I have not set forth all of the facts and circumstances of which I am aware.

investigations, I have become familiar with methods of determining whether a child is a minor. I have also gained expertise regarding the use of computers in connection with crimes against children. I have received training relating to the use of computers by offenders and gained expertise through participating in numerous cases in which computers were used to facilitate crimes against children.

2. I am familiar with the information contained in this affidavit based on my own personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

INTRODUCTION

3. This affidavit is in support of an application to search the SUBJECT ITEMS. For the reasons set forth below, I believe there is probable cause to believe that computerized and other information is contained within the SUBJECT ITEMS that is evidence or fruits or instrumentalities of offenses relating to

the aggravated sexual abuse of children, in violation of Title 18, United States Code, Section 2241(c), possession, access with intent to view, transportation, receipt, distribution, reproduction attempted production and conspiracy to produce sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2251, 2252 and 2252A, and enticement of a minor to engage in illegal sexual activity, in violation of Title 18, United States Code, Section 2422(b). The items to be searched for and seized are specifically described in Attachment B to this affidavit which is incorporated herein.

THE SUBJECT ITEMS

4. The SUBJECT ITEMS are: ONE APPLE LAPTOP, SERIAL NO. 7393759V7XJ, ONE SONY DIGITAL CAMERA, SERIAL NO. 0124465, ONE 8GB SD CARD, ONE USB MEMORY STICK, ONE BLACK APPLE IPHONE, all of which were seized from BEBARS BASLAN and KRISTEN HENRY on March 19, 2013 at the time of their arrest in Jersey City, New Jersey. The SUBJECT ITEMS are currently located at the offices of the United States Attorney's Office for the Eastern District of New York, 271 Cadman Plaza East, Brooklyn, New York.

PROBABLE CAUSE

5. On or about February 13, 2013, a Confidential Source ("CS 1") reported to the FBI that an associate of CS 1, BEBARS BASLAN and BASLAN's girlfriend, KRISTEN HENRY, possess child pornography and were preparing to sexually exploit children. CS 1 indicated that BASLAN told CS 1 that BASLAN and HENRY planned on opening a babysitting business as a cover to drug and sexually abuse children. CS 1 further stated that in order to protect himself BASLAN wanted collateral he could use to blackmail HENRY, so BASLAN had asked CS 1 to provide a one-and-a-half-year-old child that is known to CS 1 ("VICTIM 1") to BASLAN so HENRY could be photographed giving oral sex to VICTIM 1. CS 1 also stated that BASLAN indicated he obtained child pornography from Internet newsgroups. Prior to February 13, 2013, CS 1 was not a Confidential Source of the FBI. The information provided by CS 1 has been corroborated by subsequent recordings as discussed below. CS 1 may face criminal charges in the future and is cooperating, in part, with the hope of reducing his ultimate sentence.

6. Following this meeting, CS 1 made numerous consensually recorded telephone calls with BASLAN at the direction of the FBI. CS 1 recorded the following

conversations, among others, excerpted portions of which are provided in sum and substance and in part below:

- a. On February 24, 2013 at approximately 6:30 p.m., CS 1 had a conversation with BASLAN over the telephone, which CS 1 recorded at the direction of the FBI, regarding BASLAN's plans to take pictures of HENRY engaging in sexual contact with VICTIM 1. During the conversation, BASLAN and CS 1 had the following exchange.

CS 1: What do you mean, like what do you want, what do you want her to do?

BASLAN: Just like, I don't know, lick, suck, whatever. Nothing big. Just her holding a phone by herself taking a picture. Why?

CS 1: Like her holding.

BASLAN: I want to take a picture and make it seem as if she took it by herself and we're not there.

CS 1: Uh-huh.

BASLAN: Like as if you dropped him off to babysit, she took a picture and I found it.

CS 1: I see what you're saying, but what I'm concerned with is, um, how, like, no penetration.

BASLAN: No. No. Nothing like that. Due, no. Just her and him.

CS 1: But what is she doing with her and him.

BASLAN: Blow.

Later during the conversation, BASLAN stated the following:

BASLAN: I don't want to have any interaction with him. I think it will be hot seeing her

. . .

I think it will be hot watching her blowing. That's it. Does that bother you?

Later during the conversations, BASLAN stated the following:

BASLAN: I want to make a little video of her blowing whatever, him wouldn't even know what was going on. And then that's it. If, after we make the video, you and me want to take a round at her, whatever, ah, like fuck her while she's blowing him and whatever, just to get turned on, I'm fine with that. I, for me, I just want it more for safety because I have something else planned for us. But I want some, I have something else planned for us, but I want to have some safety thing on her and then she has actually access, I'll tell you in person, but she has access to the next thing. But I just want to make sure I secure her because [unintelligible].

- b. At approximately 6:40 pm on the same day, BASLAN and CS 1 had another telephone conversation, which CS 1 recorded at the direction of the FBI. During the conversation, BASLAN stated that HENRY is "dying for

this," referring to the plan to have HENRY sexually abuse VICTIM 1. Later in the conversation, CS 1 expressed concerns of the "mental stability" of VICTIM 1, and BASLAN stated "if it's one minute he won't even know what's going on," and "I think what we can do is also cover up his face really quick, as if you like pretend you're tickling him or something, and she just takes the pose, she doesn't actually do anything, she just takes the pose. You understand what I mean?" BASLAN later stated "I'm not looking for an actual thing to happen. I'm just looking for the pose of it. You could for all I care be on the other side, like, covering his face or whatever, and she just can do two licks or whatever and he wouldn't know the difference between her cleaning him or her doing whatever". After some additional discussion, the call was ended by CS 1.

- c. At approximately 6:55 pm on the same day, BASLAN and CS 1 had another telephone conversation, which CS 1 recorded at the direction of the FBI. They had a discussion of what HENRY would do with VICTIM 1. BASLAN indicated that HENRY did not need to perform

the act and that it just needs to look like it is being performed. Shortly after this, BASLAN stated the following:

BASLAN: Exactly. That's the only reason for it. There is no, for me, the fact that he, the genderwise, does not appeal to me whatsoever. Nothing. Except that's the easiest one to have right now. The first one to have the picture and with the babysitting thing, it's something that, I, she has to arrange, so I have to just make sure that we're settled before hand. That's it. The act itself does not even have to be performed. It has to look like on phone that it is.

Later during the conversation, BASLAN and CS 1 had the following exchange:

BASLAN: I'm not looking for it to be anything physical and the other stuff is all going to be when the person is passed out, [text omitted]

CS 1: Like you're saying, like with the babysitting gigs, we're going to do the roofies, so it won't affect them.

BASLAN: Exactly, they're going to be, yeah, yeah, well, we're going to, trust me, all what I'm doing nothing is going to be, no memories, nothing. It's just you know.

Later during the conversation, BASLAN stated that HENRY is "dying for me to have a baby with her for us to whatever." CS 1 then asked "The two of you

together to have your own kid and then you raise it in a sexual, like, upbringing kind of a thing?" BASLAN responded, "Right." Later during the conversation, BASLAN and the CS 1 had the following exchange concerning HENRY's interest in an eight-year-old girl (VICTIM 2)² known to CS 1:

BASLAN: Like the thing with [PARENT 1], she's [HENRY] been begging me every single week. Like, I don't know what to tell you, it's been annoying with me, every single five minutes she brings it up because she wants to do it.

CS 1: What do you mean, babysit [PARENT 1's] kid?

BASLAN: Yes.

CS 1: She's, she's, she's seen him before?

BASLAN: Yeah, oh yeah yeah, and she wants to, you know, just go Dramamine, you know, the allergy thing and do it, um, and then you know just it knocks them out a little bit.

CS 1: What do you mean?

BASLAN: You know, Dramamine, the allergy medicine. It knocks you out, when you're a kid.

CS 1: It won't, it won't, um, cause any like.

BASLAN: No. It's kid's Dramamine, it's meant for, if you get car sick, you take it and you get knocked out.

² VICTIM 2's parent is referenced in the complaint as PARENT 1.

CS 1: So, she wants to give, who [VICTIM 2]?

BASLAN: Yeah, [unintelligible].

BASLAN stated that HENRY wanted to use "kids Dramamine" to drug the children and that they could "rub it in their mouth a little bit".

7. Following these conversations, BASLAN and CS 1 had additional conversations in which they agreed that BASLAN, HENRY, CS 1, VICTIM 1 and an additional 3-month-old boy³ (VICTIM 3) would meet at a New Jersey hotel, so that HENRY could take sexually explicit photographs with VICTIM 1.

8. On March 7, 2013, CS 1, who was equipped by the FBI with electronic monitoring devices including audio recorders and a video recorder, met with BASLAN and HENRY at the residence shared by BASLAN and HENRY. During the meeting, CS 1 recorded BASLAN and HENRY discussing the plan to babysit children so that BASLAN and HENRY could sexually molest them. During the meeting, BASLAN, HENRY and CS 1 had the following exchange regarding HENRY's ability to obtain babysitting jobs:

³ VICTIM 3's age is often incorrectly identified as two months old during the course of recorded conversations.

CS 1: I don't even know, I'd have to put my mind to working something like that out. I couldn't do that. That would be, like, Kristen's problem that's the only way something like that would work out because guys would be like, yeah hi I'm a babysitter.

BASLAN: No, no, no, she has [PARENT 2] that she has [unintelligible].

HENRY: I have, like.

CS 1: [PARENT 2] has, um, a twelve-year-old daughter and a nine-year-old daughter?

BASLAN: Something like that.

HENRY: Y'all know I did work in schools [unintelligible], I worked with kids.

CS 1: So you have references, so it'll look good.

HENRY: Oh yeah, I have excellent references.

Later during the meeting, HENRY and CS 1 had the following exchange:

CS 1: Where'd you babysit? Was this in Rochester? In Buffalo, whatever?

HENRY: Yeah, I've babysat, since I was like fifteen, thirteen, fourteen.

CS 1: So, you're, you've got like crazy references.

HENRY: Yeah.

CS 1: So it'll look good, that'll be very good.

HENRY: Our little scheme.

CS 1: Um, here's a crazy question, have you ever done this before?

HENRY: No.

CS 1: You've never done this before.

HENRY: No, like, I always remember [unintelligible], but I like wouldn't admit it to myself. When I was young I used to have, um, I wouldn't even admit to myself that it was like fantasies, they were just subconscious, you know, scenarios. And um, he was like the first human I admitted it to. This is how it came out, cause we both started kind of like, I don't even remember how it, like, got out there, but both of us were like, yeah, you know, I kind of like this, just have, it turned into this.

9. Later during the meeting, BASLAN used his computer to access child pornography which he played on his television while HENRY and CS 1 were present. Some of the child pornography videos were captured on the video recording device provided to CS 1 by the FBI. The videos appeared to depict prepubescent girls being vaginally and orally penetrated by adult men's penises. Some of the videos had sound, and the children can be heard. HENRY commented regarding one of the child pornography videos that it was the "hottest one." BASLAN described to CS 1 that the child pornography in his residence can be accessed on his iPad, iPhone, and television, and that the devices were accessing the child pornography from a central location. BASLAN told CS 1 that he uses encryption that he created and that his files are "unhackable".

10. CS 1 later canceled the planned meeting in New Jersey with BASLAN and HENRY. The meeting was later reset for March 19, 2013 at hotel in Jersey City, New Jersey.

11. On March 18, 2013, CS 1, who was equipped by the FBI with electronic monitoring devices including audio recorders and a video recorder, met with BASLAN. During the conversation, they discussed plans regarding their meeting in New Jersey. CS 1 indicated that he would be bringing VICTIM 1, VICTIM 2, and VICTIM 3. During the course of the conversation, BASLAN and CS 1 had the following exchange:

CS 1: What's the game plan? What's Kristen into?

BASLAN: She's going to come and do whatever we tell her to do. That's it.

CS 1: She's going to do whatever we tell her to do? Really, it's like that?

BASLAN: Well, yeah.

CS 1: So, we're going to have a whole lot of fun?

BASLAN: Yeah. That's really about it. We're just going to have fun and then I don't know. We'll finish having fun and we'll come back.

CS 1: Yeah, I have to leave there because I have work in the morning.

BASLAN: We won't stay there overnight. Because we don't want to risk her waking up and seeing us. Once we're done, we'll leave.

CS 1: I'm not kicking you out or anything.

BASLAN: No, no, no, I wouldn't want to. I mean why should she even see us.

CS 1: Yeah, exactly, how am I going to explain that?

BASLAN: Right, right. And I was thinking that when we do that deed, we'll all wear, like, ski masks and then we'll have a movie with ski masked robbers running playing in the living room, so if she gets scared we just pull out turn off the light, disappear and then you'll be sitting on the couch watching a ski mask movie. Oh honey what happened did this movie get in your head again?

CS 1: Um, you're going to bring the camera, by the way?

BASLAN: Of course.

CS 1: The HD one, right?

BASLAN: Of course, I have a DSLR HD I'm going to bring, fully charged, fully loaded.

CS 1: What's DLL-uh-uh?

BASLAN: It's like a photo camera that takes videos.

CS 1: But no faces.

BASLAN: Of course not, well except Kristen.

CS 1: Ok. Not even accidentally, Alright?

BASLAN: Don't worry, man, like I said, just Kristen's and my dick's face.

Later during the conversation, BASLAN and CS 1 had the following exchange:

BASLAN: You know I was just saying, you should stop by before you leave to take that one shot with [VICTIM 1] because that's explainable

in my bedroom, or not [VICTIM 1] the younger one.

CS 1: [VICTIM 3]?

BASLAN: Just for like [unintelligible].

CS 1: [VICTIM 3]'s only like, not even two months old.

BASLAN: I know, that's what I'm saying, she can change his diaper and she can, we can take that picture on the bed, so that kind of like makes sense why she has the picture. Then you leave get [VICTIM 2], leave and we'll follow you to, we'll wait a little bit to.

CS 1: And you'll follow me to the, um.

BASLAN: Right, because that makes more sense, you know I want to take it with her camera versus the other camera, but I don't want to have too many cameras on me.

Later during the conversation, BASLAN and CS 1 had the following exchange:

BASLAN: Like I said, we can take it easy tomorrow, just get, I'm going to bring her and we get [VICTIM 2] take a few pictures, something like that or whatever and we just, that would be our first time and we'll take it further next one.

CS 1: How far do you want to go?

BASLAN: Not too far. Take pictures. Touch and then go down on her. That's pretty much what I want out of it.

CS 1: You just want to go down on her?

BASLAN: Yeah. Nothing else, I mean.

CS 1: For now?

BASLAN: Because I don't know anything else about her, she's you know, what else can I do, we'll figure out as we get more advanced in this but the first time around, that's more than enough.

Later during the conversation, BASLAN and CS 1 had the following exchange:

CS 1: I don't know how I feel about penetration and shit like that.

BASLAN: If we had better drugs and she's a different person, I wouldn't have a problem with it?

CS 1: What do you mean by different drugs?

BASLAN: Different person, better drugs, different situation, whatever.

CS 1: You if it wasn't [text which may tend to identify VICTIM 2 has been omitted].

BASLAN: No, it's not so much about that. It's just more like, if she was a kid that's willing, it wouldn't be a problem per se.

CS 1: How the fuck do you know a kid that's willing? How do you pick that up? Like what?

BASLAN: Sure you can pick that up. A lot of kids do, I mean I was in, when I was their age, I was willing. I knew a lot of, from the stuff that I've seen online and stuff, there's a lot more stuff online where the girls is like whoa go for it, more than even the guy.

CS 1: Really?

BASLAN: Yeah. Because from my few experiences, I've never acted out anything but more than once

I've had the situation where the kid is totally willing.

CS 1: I wouldn't, I'd be too afraid if they were awake.

BASLAN: If the kid is willing, though, they, it wouldn't be your problem.

CS 1: It's not a problem?

BASLAN: No, because it wouldn't, they're going to want it. Trust me. Next time they see you, they're going to be like attacking you wanting more.

CS 1: Really?

BASLAN: Yeah. So. But still. But in a different situation you could have anal with a kid and it wouldn't be a problem. It wouldn't leave any marks or anything. Then just vaginally you can't do because that.

CS 1: Will tear?

BASLAN: Yeah, but anal, yeah.

CS 1: Anal you can have, vaginal you can't?

BASLAN: One thing I noticed, all the guys all do anal first, they don't do vaginal unless the kid is willing and it's that kind of a situation.

CS 1: Because, that's proof?

BASLAN: Yeah, you can see that immediately. Anal you can't.

Later during the conversation, BASLAN and CS 1 had the following exchange referring to the plans to sexually abuse VICTIM 3:

BASLAN: But tomorrow, definitely no penetration, we'll go the line where we you know, take pictures and video and that'll be cool.

CS 1: Alright, I'm.

BASLAN: If you want to do that, you don't have to bring, just bring [VICTIM 1] here for the picture.

CS 1: Right.

BASLAN: Just park your car, I'll bring him inside, take the picture, send her, send him out and then, you're good to go.

CS 1: [VICTIM 1] or [VICTIM 3]?

BASLAN: [VICTIM 3], I mean, [VICTIM 3]

CS 1: The two month old.

BASLAN: Yeah, the younger one, I keep mixing them up. The younger one.

CS 1: [VICTIM 3] is the two month old. [VICTIM 1] is the 16-month.

BASLAN: For the picture, for the picture it doesn't make a difference.

CS 1: What do you mean?

BASLAN: The younger one.

CS 1: It doesn't matter if he's a year and a half or two months, that's what you're saying?

BASLAN: Yeah, yeah, exactly. And then, that's it. What we're going to have to do, I'm going to have her the camera with her hand in the position that it's the right angle. Click click click click.

CS 1: She's just going to take the pictures herself?

BASLAN: No I'm going to take them, but I'm going to have her hand behind the camera, make sure the picture is covered, and just going to have her hold her hand.

CS 1: As if she, simulate as if she's the one taking the picture.

BASLAN: Yup.

Later during the conversation, BASLAN and CS 1 had the following exchange, which is relayed in sum and substance and in part.

CS 1: Did you have this other one lined up?

BASLAN: Yeah, I'm working on it.

CS 1: The babysitting gig.

BASLAN: Yeah, she's going to meet her in a couple of days to just to see, they meet Kristen, just to see

Later during the conversation, BASLAN indicated that VICTIM 2 is more of a "stepping stone" and that he will "take a lot of pictures and videos." BASLAN also stated: "We'll have a good amount of pictures and videos of [VICTIM 2] herself and then we can just use it as jerk-off material or whatever."

12. On March 19, 2013, CS 1 placed a recorded call to BASLAN at the direction of the FBI and indicated that he would not have time to bring VICTIM 1 and VICTIM 3 to BASLAN's residence, so that HENRY could take a sexually explicit photograph with VICTIM 3. BASLAN and the CS 1 agreed that CS 1

would go by BASLAN's residence to pick up the drugs that would be used to incapacitate VICTIM 2, then BASLAN, HENRY and CS 1 would meet at the New Jersey hotel. During recorded conversations that day, BASLAN and CS 1 also agreed on a code word that would indicate that CS 1 had VICTIM 1, VICTIM 2, and VICTIM 3 at the hotel and that BASLAN and HENRY could travel to New Jersey to sexually abuse them.

13. In the early evening of March 19, 2013, CS 1 drove to BASLAN's residence, which was under surveillance by law enforcement. CS 1 was equipped by the FBI with electronic monitoring devices including audio recorders and a video recorder. After CS 1 arrived, BASLAN indicated to CS 1 that HENRY would be arriving with the drugs. Shortly after that, law enforcement officers observed HENRY driving back to BASLAN's residence. BASLAN, HENRY, and CS 1 then went inside BASLAN's residence and had a short discussion regarding the drugs. During the meeting, HENRY provided CS 1 with children's Benadryl and orange juice. CS 1 left as soon as the meeting concluded and immediately met with law enforcement officers, to whom CS 1 provided the drugs that he/she had received from HENRY.

14. Later in the evening, at the direction of the FBI, CS 1 placed a recorded call to BASLAN and provided the code word indicating he had obtained VICTIM 1, VICTIM 2, and VICTIM 3. CS 1 also indicated the address of the hotel and room number.

15. Later in the evening, law enforcement officers conducting surveillance on BASLAN's residence observed BASLAN's car leave the area.

16. At approximately 9:15 p.m., BASLAN and HENRY arrived at the hotel in Jersey City, New Jersey. Shortly after that they arrived at the room, whose number CS 1 had previously provided to BASLAN. CS 1 let them into the room. Law enforcement officers then entered the room and arrested BASLAN and HENRY. Unbeknownst to BASLAN and HENRY, no children were present in the room. At the time of BASLAN's arrest, BASLAN was carrying a backpack and HENRY was carrying a purse. During a search of the backpack and purse incident to BASLAN and HENRY's arrests, agents discovered the SUBJECT ITEMS.

17. SUBJECT ITEMS 1-5, 7 and 8 were found in the backpack. SUBJECT ITEMS 6, 9-11 were found in the purse.

TECHNICAL TERMS

18. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders,

even when the devices communicating with each other are in the same state.

- c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

DEFINITIONS

19. The following definitions apply to this Affidavit and Attachment A to this Affidavit:

- a. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit

conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

- b. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).
- c. "Sexually explicit conduct" means actual or simulated
 - (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).
- d. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related

to or operating in conjunction with such device[.]”

It includes cellular telephones

e. “Computer hardware,” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); and peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as modems, routers, cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

f. “Computer software,” as used herein, is digital information which can be interpreted by a computer and

any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

g. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

h. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

i. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

j. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital

data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

k. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate

the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

1. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

- m. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- n. Pager: A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.
- o. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to,

writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, drives, or electronic notebooks and tablets, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

SUBJECT ITEMS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

20. Based on my training and experience, I am aware that SUBJECT ITEMS 2 and 9 are digital cameras and that SUBJECT ITEMS 5 and 6 are mobile computers and can function as wireless telephones, digital cameras, GPS, and PDAs.

21. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

22. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

23. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used,

what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

24. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

25. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the SUBJECT ITEMS because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since

been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

- b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files,

user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information

stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to receive or distribute child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I

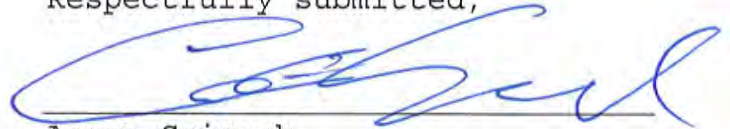
believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

26. *Anytime of the Day or Night.* The SUBJECT ITEMS are currently lawfully in the possession of the government. As a result, the search of the SUBJECT ITEMS at any time of the day or night would not inconvenience anyone. The government, therefore, requests that the search of the SUBJECT ITEMS may be conducted at any time of the day or night.

CONCLUSION

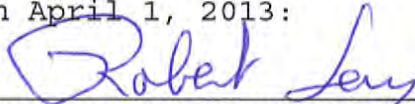
27. I submit that this affidavit supports probable cause for a warrant to search the ITEMS described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,



Aaron Spivack
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on April 1, 2013:



THE HONORABLE ROBERT M. LEVY
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be Searched

The SUBJECT ITEMS are ONE APPLE LAPTOP, SERIAL NO. 7393759V7XJ ("SUBJECT ITEM 1"), ONE SONY DIGITAL CAMERA, SERIAL NO. 0124465 ("SUBJECT ITEM 2"), ONE 8GB SD CARD ("SUBJECT ITEM 3"), ONE USB MEMORY STICK ("SUBJECT ITEM 4"), and ONE BLACK APPLE IPHONE ("SUBJECT ITEM 5"), ONE WHITE APPLE IPHONE ("SUBJECT ITEM 6"), ONE 32 GB SD CARD ("SUBJECT ITEM 7"), ONE SKY LINK CDMA MODEM ("SUBJECT ITEM 8"), ONE SONY DIGITAL CAMERA, SERIAL No. 7080101 ("SUBJECT ITEM 9"), ONE GREY NOTEBOOK, WITH COVER READING "SECRET MAGIC SPELLS" ("SUBJECT ITEM 10"), and ONE 4 GB SD CARD ("SUBJECT ITEM 11") (collectively referred to as the "SUBJECT ITEMS")

ATTACHMENT B

Particular Things to be Seized

ITEMS TO BE SEIZED FROM THE SUBJECT ITEMS, all of which constitute evidence or instrumentalities of violations of Title 18, United States Code Sections 2241(c), 2251, 2252, 2252A and 2422(b):

1. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the production, possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2251, 2252 and 2252A, in any form wherever they may be stored or found;

2. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

3. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

4. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:

a. correspondence, including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or relating to the enticement of minors to engage in illegal sexual activity; and

b. ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

5. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.

6. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

7. Records or other items which evidence ownership or use of computer related equipment, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

8. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct or the enticement of minors to engage in illegal sexual contact.

9. Address books, names, lists of names and addresses of individuals believed to be parents or guardians of minors.

10. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be parents or guardians of minors.

11. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.

12. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

13. All documents, text messages, "chat," or instant messages, call logs, and any other electronically-stored data (whether on cellular telephones or elsewhere) relating to conspiracy to produce child pornography or attempts to produce child pornography or enticement of minors to engage in illegal sexual contact or aggravated sexual abuse of children.

14. Evidence of who used, owned, or controlled any of the SUBJECT ITEMS at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence. User attribution information (i.e. files and other data such as chats or e-mails) relevant to the trading of child pornography. Such information tends to show the identity of the person using the computer near the time of the criminal activity;

15. Evidence of software that would allow others to control the computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

16. Evidence of the lack of such malicious software;

17. Evidence of the attachment to the computer of other storage devices or similar containers for electronic evidence;

18. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer;

19. Evidence of the times the SUBJECT ITEMS were used;
20. Passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT ITEMS;
21. contextual information necessary to understand the evidence described in this attachment.

If any materials protected by the Privacy Protection Act, 42 U.S.C. § 2000aa are inadvertently seized, all efforts will be made to return these materials to their authors as quickly as possible.

22. Records and things evidencing the use of any IP address, including:

- a. records of Internet Protocol addresses used;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections , 2241(c), 2251, 2252, 2252A and 2422(b) .

Definitions

- a. "Child Erotica," as used herein, means materials and items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene and that do not necessarily depict minors in sexually explicit poses or positions.

- b. "Child Pornography," as used herein, includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer generated image that is, or is

indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct (see 18 U.S.C. §§ 2252 and 2256(2)).

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital, oral genital, or oral anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

e. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

f. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); and peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as

cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

g. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

h. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

i. "IP Address" as used herein, the IP Address or Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

j. "Wireless telephone": A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

k. "Digital camera": A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

l. "Portable media player": A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include

various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

p. "GPS": A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

q. "PDA": A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and

presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

r. "Tablet": A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

s. "Pager": A pager is a handheld wireless electronic device used to contact an individual through an alert, or a numeric or text message sent over a telecommunications network. Some pagers enable the user to send, as well as receive, text messages.

t. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).